Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

PENDING CLAIMS

1-19. (Cancelled)

20. (Currently Amended) A method for managing sensitive data, comprising:

storing the sensitive data in an encrypted file with an encrypted digital signature and an encrypted user signature; and

storing a temporary, encrypted copy of the file;

decrypting a proper subset of the temporary, encrypted copy of the file in a function local to a trusted application when performing a read operation; and

decrypting a proper subset of the temporary, encrypted copy of the file in a function local to a trusted application when performing a write operation;

updating the digital signature of the encrypted, temporary file, using the proper subset and a data subset to be written to the ~~encrypted, temporary file~~ temporary, encrypted copy of the file;

encrypting the data subset to be written to the ~~temporary, encrypted file~~ temporary, encrypted copy of the file and writing said data subset to the ~~temporary, encrypted file~~ temporary, encrypted copy of the file;

using the encrypted digital signature and encrypted user signature to authenticate the ~~encrypted, temporary copy of the file~~ temporary, encrypted copy of the file; and

updating the file with the ~~encrypted,~~ temporary, encrypted copy of the file when performing a file close operation.

21. (Currently Amended) A method for managing sensitive data, comprising:

a) a file creation step comprising:

creating a file containing sensitive data;

calculating a digital signature and a user signature for the file;

storing the digital signature and the user signature in the file together with the sensitive data;

encrypting the file containing the sensitive data, the digital signature and the user signature to produce an encrypted file;

creating and storing a temporary copy of the encrypted file; and

b) a file operation step comprising:

performing an input-output operation on a proper subset of the encrypted file without the need to decrypt the entire file;

the file operation step characterized by comprising:

decrypting a proper subset of the temporary copy in a function local to a trusted application when performing a read operation;

decrypting a proper subset of the temporary copy in a function local to a trusted application when performing a write operation;

updating the digital signature of the temporary copy, using the decrypted proper subset and a data subset to be written to the temporary copy;

encrypting the data subset to a be written to a temporary copy;

writing the encrypted data subset to the temporary copy;

encrypting the digital signature and the user signature;

adding the encrypted digital signature and the encrypted user signature to the temporary copy to authenticate ~~it~~ the temporary copy ; and

updating the encrypted file with the thus modified temporary copy when performing a file close operation.

22. (New) A method for managing sensitive data, comprising:

a) a file creation step comprising:

creating a file containing sensitive data;

calculating a digital signature and a user signature for the file;

storing the digital signature and the user signature in the file together with the sensitive data;

encrypting the file containing the sensitive data, the digital signature and the user signature to produce an encrypted file; and

b) a file operation step comprising:

passing the encrypted file to a local function having a syntax to accept at least a file name parameter, a user signature parameter, and a user key parameter, the local function containing

encryption instructions, decryption instructions, and authentication instructions, all instructions being performed at the local function level.

23. (New) A method of developing a trusted application, comprising:

installing a library of functions for performing input-output operations, each function in the library of functions having a syntax to accept at least a file name parameter, a user signature parameter, and a user key parameter, the local function containing encryption instructions, decryption instructions, and authentication instructions, all instructions being performed at the local function level; and

developing a trusted application by using the library of functions by installing a standard library that includes at least one standard input/output function for file/streams and replacing the at least one standard input/output function for file/streams with at least one corresponding functions for performing input-output operations from the library.

24. (New) A method for managing sensitive data, comprising:

a) a file creation step comprising:

creating a file containing sensitive data;

calculating a digital signature for the file;

storing the digital signature in the file together with the sensitive data; and encrypting the file containing the sensitive data and the digital signature to produce an encrypted file; and

b) a file operation step comprising;

performing an input-output operation on a subset of the encrypted file without the need to decrypt the entire file;

the file operation step comprising:

decrypting the subset of the file in a function local to a trusted application when performing a read operation;

decrypting the subset of the file in a function local to a trusted application when performing a write operation;

updating the digital signature of the file, using the decrypted subset;

encrypting the subset to be written to the file;

writing the encrypted subset to the file;

encrypting the digital signature; and

adding the encrypted digital signature to the file to authenticate the file.

25. (New) A method for managing sensitive data in a distributed computer system having at least one trusted machine connected to a plurality of untrusted machines, the method comprising:

a) an installation step comprising:

installing a trusted application on the plurality of untrusted machines, the trusted application being compiled using a library of functions for performing input-output operations, each function in the library of functions having a syntax to accept at least a file name parameter, a user signature parameter, and a user key parameter, the local function containing encryption instructions, decryption instructions, and authentication instructions, all instructions being performed at the local function level;

b) a file creation step comprising:

creating a file containing sensitive data;

calculating a digital signature and a user signature for the file;

storing the digital signature and the user signature in the file together with the sensitive data;

encrypting the file containing the sensitive data, the digital signature and the user signature to produce an encrypted file;

c) a file operation step comprising:

passing the encrypted file to the trusted application;

performing the input-output operations on the encrypted file; and

d) an output step comprising:

sending output based on the encrypted file to the trusted machine.

26. (New) A computer readable medium comprising computer code for causing a computer to perform:

a) a file creation step comprising:

creating a file containing sensitive data;

calculating a digital signature and a user signature for the file;

storing the digital signature and the user signature in the file together with the sensitive data;

encrypting the file containing the sensitive data, the digital signature and the user signature to produce an encrypted file; and

b) a file operation step comprising:

passing the encrypted file to a local function having a syntax to accept at least a file name parameter, a user signature parameter, and a user key parameter, the local function containing encryption instructions, decryption instructions, and authentication instructions, all instructions being performed at the local function level.